Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2025-64155: Critical FortiSIEM RCE with Public Exploits Available

Date of Publication	Admiralty Code	TA Number
January 15, 2026	A1	TA2026014

Summary

First Seen: January 13, 2026
Affected Products: Fortinet FortiSIEM
Impact: CVE-2025-64155 is a critical remote command injection vulnerability in Fortinet FortiSIEM that allows unauthenticated attackers to execute arbitrary OS commands via the phMonitor service (TCP port 7900). With a CVSS score of 9.8, successful exploitation can result in full system compromise, including privilege escalation and access to sensitive security data. Multiple on-prem FortiSIEM versions are affected, while FortiSIEM Cloud is not. Public proof-of-concept exploits and demonstrated threat actor interest significantly increase risk for exposed deployments. Immediate patching and network access restrictions are strongly recommended.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-64155	Fortinet FortiSIEM OS Command Injection Vulnerability	Fortinet FortiSIEM	☒	☒	✓

Vulnerability Details

#1

CVE-2025-64155 is a critical remote command injection vulnerability affecting Fortinet FortiSIEM, a widely used Security Information and Event Management (SIEM) platform. Disclosed on January 13, 2026, the flaw is caused by improper sanitization of user-supplied input passed to operating system commands. The vulnerability resides in the phMonitor service (port 7900), which accepts crafted network requests without authentication, allowing remote exploitation.

#2

The impact is severe with a CVSS score of 9.8. A successful exploit allows an attacker to execute arbitrary OS commands on the underlying FortiSIEM system, potentially resulting in full system compromise including privilege escalation to root, access to sensitive logs, credentials, and security telemetry. No privileges or user interaction are required for exploitation. Affected versions include FortiSIEM 7.4.0, 7.3.0 - 7.3.4, 7.1.0 - 7.1.8, 7.0.0 - 7.0.4, and 6.7.0 - 6.7.10. FortiSIEM Cloud is not affected.

#3

Public proof-of-concept exploits have been released, increasing the likelihood of exploitation, especially for internet-exposed or poorly segmented deployments. At the time of disclosure, there was no evidence of active exploitation in the wild; however, leaked Black Basta ransomware group chat logs from earlier in 2025 showed discussions about FortiSIEM vulnerabilities, indicating threat actor interest in targeting these systems.

#4

Fortinet has released security patches to address the issue, with fixed versions being 7.4.1, 7.3.5, and 7.2.7. Until patching is completed, organizations should restrict network access to port 7900, monitor for suspicious connection attempts, and review logs for indicators of compromise. Given FortiSIEM's role in security monitoring, exploitation of this vulnerability poses a high strategic risk to affected environments.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-64155	Fortinet FortiSIEM (7.4.0, 7.3.0-7.3.4, 7.2.0-7.2.6, 7.1.0-7.1.8, 7.0.0-7.0.4, 6.7.0-6.7.10)	cpe:2.3:a:fortinet:fortisiem:*:*:*:*:*:*:*:*	CWE-78

Recommendations

Apply Security Patches Immediately: Organizations running affected versions of FortiSIEM should prioritize the installation of security updates released by Fortinet as the primary remediation measure. FortiSIEM 7.4.x users should upgrade to version 7.4.1 or above, FortiSIEM 7.3.x users should upgrade to version 7.3.5 or above, FortiSIEM 7.2.x users should upgrade to version 7.2.7 or above, and FortiSIEM 7.1.x users should upgrade to version 7.1.9 or above. Users on FortiSIEM 7.0.x and 6.7.x branches should migrate to a fixed release as patches for these older branches may not be available.

Implement Network Access Restrictions: If immediate patching is not feasible, implement compensating controls by restricting network access to the phMonitor service port (TCP port 7900) as recommended by Fortinet. This can be accomplished through firewall rules, network segmentation, or access control lists that limit connectivity to the phMonitor port only from trusted administrative networks and authorized FortiSIEM components such as Collectors that legitimately require this access.

Enhance Network Monitoring and Detection: Deploy network-based detection capabilities to identify exploitation attempts targeting the phMonitor service. Monitor for anomalous TCP connections to port 7900, particularly from external or untrusted network segments. Implement alerting for any connections to this port that do not originate from known and authorized FortiSIEM components within your environment.

Conduct Forensic Log Analysis: Review the FortiSIEM logs located at /opt/phoenix/log/phoenix.log for indicators of potential exploitation attempts. This log file records the contents of messages received by the phMonitor service, and exploitation attempts will appear as log entries containing "PHL_ERROR" with malicious URL patterns and file paths indicating attempts to abuse the elastic_test_url.sh functionality. Look specifically for entries containing unusual curl arguments, external IP addresses, or references to sensitive system files.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Persistence	T1053: Scheduled Task/Job	T1053.003: Cron
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Defense Evasion	T1222: File and Directory Permissions Modification	
Collection	T1005: Data from Local System	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
Impact	T1489: Service Stop	

Patch Details

Upgrade Fortinet FortiSIEM to the fixed versions 7.4.1, 7.3.5, 7.2.7 and 7.1.9 or above.

Link:
https://www.fortiguard.com/psirt/FG-IR-25-772

References

https://www.esentire.com/security-advisories/critical-fortinet-fortisiem-vulnerability-cve-2025-64155-disclosed

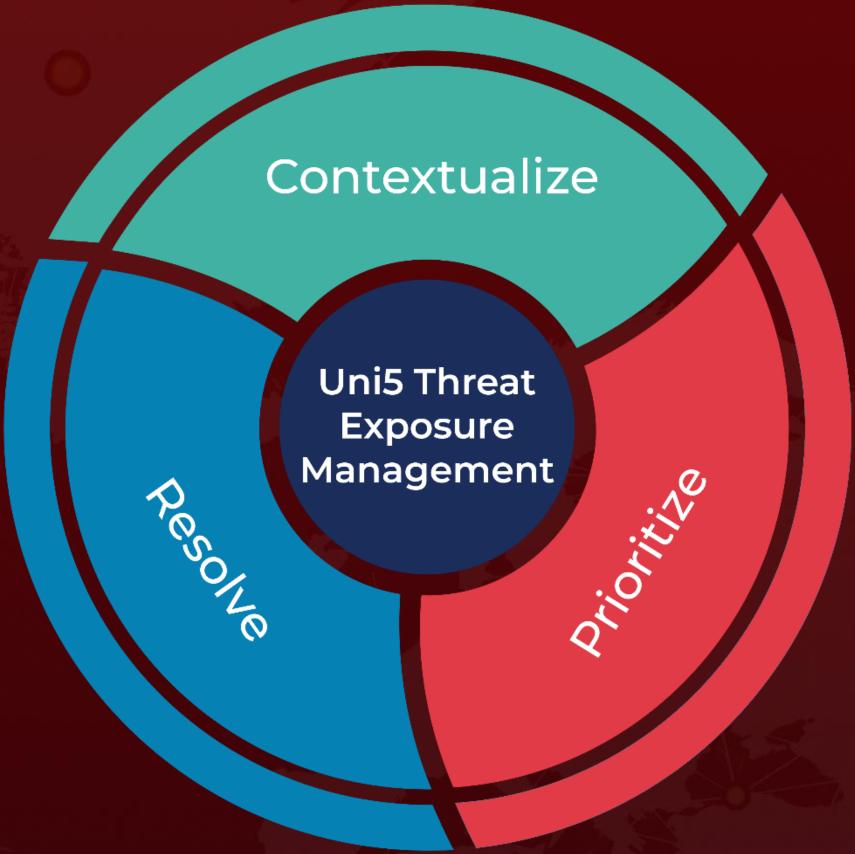
https://horizon3.ai/attack-research/disclosures/cve-2025-64155-three-years-of-remotely-rooting-the-fortinet-fortisiem/

https://github.com/horizon3ai/CVE-2025-64155

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 15, 2026 • 06:30 AM

More at www.hivepro.com